

# **EXHIBIT 7**



**VIA EMAIL**

November 22, 2023

Fish & Richardson P.C.  
1180 Peachtree Street, NE  
21st Floor  
Atlanta, GA 30309  
404 892 5005 main  
404 892 5002 fax

Reza Mirzaie  
RUSS AUGUST & KABAT  
12424 Wilshire Blvd. 12th Floor  
Los Angeles, CA 90025  
rmirzaie@raklaw.com

**Thad C. Kodish**  
Managing Principal  
[TKodish@fr.com](mailto:TKodish@fr.com)  
404 724 2792 direct

RE: *Headwater Research, LLC v. Samsung Electronics America, Inc. and Samsung Electronics Co. Ltd.*, No. 2:23-cv-00103-JRG-RSP (E.D. Tex.); Headwater Research LLC's Disclosure of Asserted Claims and Infringement Contentions

Counsel:

I write regarding deficiencies in Headwater's infringement contentions served on September 28, 2023. Headwater's contentions fail to adequately disclose discernable infringement theories for multiple asserted claim elements across the patents-in-suit. Headwater must promptly address the deficiencies detailed below and serve proper infringement contentions that comply with the Patent Local Rules to avoid any further prejudice to Samsung. Please confirm that Headwater will do so no later than November 28, 2023.

**I. Headwater's Failure to Adequately Disclose Its Infringement Theories to Samsung**

Headwater's contentions fail to comply with the disclosure requirements of P.R. 3-1, which requires Headwater to provide “[a] chart identifying specifically where each element of each asserted claim is found within each Accused Instrumentality.” In this District, the “Patent Rules demonstrate high expectations as to plaintiffs’ preparedness before bringing suit” and require plaintiffs to “set forth ‘particular theories of infringement with sufficient specificity to provide defendants with notice of infringement beyond that which is provided by the mere language of the patent [claims] themselves.’” *Connectel, LLC v. Cisco Sys, Inc.*, 391 F. Supp. 2d 526, 527-28 (E.D. Tex. 2005) (citing *STMicroelectronics, Inc. v. Motorola, Inc.*, 308 F. Supp. 2d 754, 755 (E.D. Tex. 2004)) (“[M]ore than a perfunctory submission is required. Plaintiffs . . . must explain with great detail their theories of infringement.”). Headwater’s infringement contentions fail to provide the required specificity to provide notice of how Headwater believes the accused products meet several of the asserted claim limitations, thereby rendering them impossible to decipher.

As a preliminary matter, Headwater’s infringement contentions cobble together screen shots without identifying what it is accusing in the screen shots for each claim limitation, much less explaining how the screen shots demonstrate that each claim element is present in each Accused Instrumentality. Worse yet, in many instances, Headwater removed the explanations it had added to address the defects identified in Samsung’s first motion to dismiss (Dkt. No. 28), rendering the contentions even more vague and deficient than what it pled in the First Amended Complaint. *Compare, e.g.*, Dkt. No. 31-4 at 12-13, 24 with Ex. A to Infr. Conts. re ’733 Patent



November 22, 2023  
Page 2

(the “‘733 Chart”) at 12, 23. As Headwater has affirmatively removed those explanations from its infringement contentions, our understanding is that Headwater will no longer assert these theories. The theories Headwater retracted are reproduced in Appendix A to this letter.

As discussed in more detail below, Headwater fails for many limitations to identify what aspect of the accused products and systems it contends satisfies that limitation. That approach does not satisfy the standards of this district. *See, e.g., Rapid Completions LLC v. Baker Hughes Inc.*, No. 15-724, 2016 WL 3407688, at \*6 (E.D. Tex. June 21, 2016) (“It is not a defendant’s job to assume how a plaintiff believes each claim element is met or to assume how a plaintiff alleges the Accused Instrumentality infringes.”); *EON Corp. IP Holdgs v. Sensus USA, Inc.*, No. 9-116, 2010 WL 346218, at \*3 (E.D. Tex. Jan. 21, 2010) (finding block quote excerpts and string cites of product specifications and reports to be “insufficient to satisfy the notice function intended by P.R.3-1 infringement contentions”); *Nat'l Oilwell Varco L.P. v. Auto-Dril, Inc.*, No. 09-85, 2010 WL 11553254, at \*3 (E.D. Tex. Dec. 2, 2010) (finding that patentee’s use of advertising brochures and website screenshots of the accused products failed to satisfy the notice requirement of P.R. 3-1(c) “because it does not indicate where in the [accused product] the asserted elements are found or describe [the patentee’s] theories of how the [accused product] meets each claim element”); *Rapid Completions*, 2016 WL 3407688, at \*5 (“[The patentee’s] inclusion of diagrams, screenshots from Defendants’ documents, and links to videos, does not automatically show that its infringement contentions are compliant with the rules. Supporting evidence in the form of block quotations from defendant’s documents or screen shots of defendant’s documents is generally insufficient to satisfy the notice function intended by P.R. 3-1 infringement contentions.”).

Additionally, specific examples of Headwater’s deficiencies with respect to each asserted patent are detailed below.

### **1. U.S. Patent No. 8,406,733**

- At least as to claim 1, Headwater fails to identify where the accused products comprise “a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network, the service control link secured by an encryption protocol and configured to support control-plane communications between the network system and a service control device link agent on the end-user device.” For example:
  - Headwater’s infringement chart reproduces the same explanations and evidence as it did in the first amended complaint, except that Headwater has removed language regarding the “service control link” and “control-plane communications” terms that it had added to overcome the deficiencies identified in Samsung’s motion to dismiss. *Compare* ‘733 Chart at 12 with ECF No. 31-4 at 12-13. As a result, Headwater’s contentions do not meet the requirements of P.R. 3-1 for at least the same reasons discussed in Samsung’s motions to dismiss. ECF No. 28 at 5-7.



November 22, 2023

Page 3

- Headwater does not identify what it accuses as a “service control device link agent” and “a service control link” in the evidence cited.
- Headwater does not identify what constitutes a “service control link” in the evidence it cites in the chart. Headwater is also silent as to how the “service control link [is] provided by the network system over a wireless access network.” Headwater merely states that the “wireless access network” limitation is met by “a wi-fi network and/or a cellular network.” ‘733 Chart at 2.
- Relatedly, Headwater has failed to explain how a service control link would be “secured by an encryption protocol and configured to support control-plane communications,” because Headwater’s chart is silent on what the “encryption protocol” is or how it secures a “service control link.” For example, for the FCM functionality, Headwater points to a screenshot indicating that the Android Transport Layer uses point-to-point encryption. ‘733 Chart at 7. But Headwater’s chart is silent on what the “encryption protocol” is or how it secures a “service control link.”
- Headwater fails to identify what the “control-plane communications” are in the evidence cited. Indeed, other than in the initial recitation of the claim limitation, Headwater **never once** uses the term “control-plane communication.”
- At least as to claim 1, Headwater fails to identify how the accused products comprise “a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier.” For example:
  - Headwater’s infringement chart reproduces the same explanations and evidence as it did in the first amended complaint, except that Headwater has removed language regarding the “service control device link agents” and “agent communication bus” terms it had added to overcome the deficiencies identified in Samsung’s motion to dismiss. *Compare* ‘733 Chart at 23 with ECF No. 31-4 at 24. As a result, Headwater’s contentions do not meet the requirements of P.R. 3-1 for at least the same reasons discussed in Samsung’s motions to dismiss. ECF No. 28 at 5-7.
  - Nowhere in its chart does Headwater identify what it is accusing as the “device agents,” the “agent communication bus,” or the “associated device agent identifier.” Headwater thus necessarily also fails to disclose its theory as to how the device agents are “communicatively coupled to the service control device link through an agent communication bus.”
- At least as to claim 1, Headwater fails to disclose how the accused products comprise “memory configured to store an encryption key, the encryption key shared between the



November 22, 2023

Page 4

service control device link agent and a service control server link element of the network system.” For example:

- Headwater does not identify “an encryption key,” “a service control device link agent,” and “a service control server link element” in the cited evidence. Indeed, other than in the initial recitation of the claim limitation, Headwater **never once** uses the term “service control server link element” in its chart.
- Headwater fails to disclose its theory as to how the “memory . . . store[s] an encryption key” and how “the encryption key [is] shared between the service control device link agent and a service control server link element.”
- Headwater provides no notice of how the encryption limitation is met. Headwater cites public materials that refer to, for example, the Knox platform encryption, secure Wi-Fi, and Android Transport Layer point-to-point encryption. It must identify where the claim elements in 1[c] exist in this evidence. Further, to the extent Headwater contends encryption in Android Transport Layer meets this limitation, Headwater must identify which infringement theory (Galaxy phones and tablets, devices that use Knox, and Tizen devices) such encryption is even relevant to.
- At least as to claim 1, Headwater’s contentions fail to disclose its theory as to how “the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element.”
  - Not only does Headwater fail to identify what it accuses as an “encrypted agent message,” but it also fails to explain how said message is received over the “service control link.” Headwater asserts that the accused devices receive messages “from a server” and that Samsung’s “push messaging servers” communicate with the “Samsung Push Service software” on the end user devices. *See* ’733 Chart at 35, 38, 45-47. But Headwater fails to explicitly identify where the evidence shows that these messages are encrypted or the “service control link” on which these messages are received. It is also not clear what Samsung’s push messaging servers and Samsung Push Service software is. Please explain where this is described in Headwater’s infringement contentions.
  - Further, Headwater asserts that applications in user devices cause notifications to be sent to user devices via Samsung’s push messaging servers and identifies “Shop Samsung” and “Galaxy Store,” but Headwater does not explain which of the three infringement theories it asserts (*i.e.*, Samsung Galaxy phones and tablets generally, Samsung’s Tizen based devices, and devices operating in Samsung Knox ecosystem) such an assertion relates to.



November 22, 2023

Page 5

- At least as to claim 1, Headwater fails to identify how the accused products, “using the encryption key, obtain a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element.”
  - Because Headwater has failed to identify the “service control device link agent,” it necessarily fails to explain how said “service control device link agent” performs decryption as claimed.
  - Headwater does not identify what it is pointing to in the cited evidence for the “particular agent identifier” and “message content,” which are the claimed components of a “decrypted agent message.”
  - Headwater fails to identify what it is pointing to for the “message content from a particular server of a plurality of servers communicatively coupled to the service control server link element” limitation.
- At least as to claim 1, Headwater fails to disclose its theory as to how the accused products, “based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus,” because Headwater has failed to identify the “service control device link agent” or the “agent communication bus” in its chart.

## 2. *U.S. Patent No. 9,198,117*

- At least as to claim 1, Headwater fails to identify “a plurality of device messaging agents, each executable on a respective one of a plurality of mobile end-user devices configured to exchange Internet data via a data connection to a wireless network” with respect to the Samsung Knox Manage ecosystem and the Tizen Push service.
- At least as to claim 1, Headwater fails to identify “a network message server supporting a plurality of secure Internet data connections, each secure Internet data connection between the network message server and a respective one of the mobile end-user devices via a device data connection to a wireless network.” For example:
  - For each accused “device messaging agent,” Headwater must identify a corresponding “network messaging server” that transmits “Internet data messages” to that particular accused “device messaging agent.” For the “device messaging agent” limitation, Headwater identifies several different features, including “the FCM client app.” ’117 Chart at 7. However, Headwater fails to identify a corresponding “network message server” that transmits messages to the accused FCM client app. As a result, even if the FCM client app constituted a “device messaging agent,” Headwater’s infringement theory would fail because Headwater



November 22, 2023

Page 6

did not identify any “network message server” that communicates with the FCM client app. Notably, this is the same deficiency Samsung identified in its motion to dismiss (Dkt. 40 at 10-11; Dkt. 42 at 1-2), but Headwater made no attempt to address it in its infringement contentions.

- Headwater does not disclose its theory as to what constitutes the “plurality of secure Internet connections,” and thus necessarily also fails to identify a network message server that supports said plurality of secure Internet data connections.
- At least as to claim 1, Headwater fails to identify a “network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications.” Headwater does not identify any requests that indicate both a corresponding mobile end-user device and an application. Headwater also fails to identify a “network message server” that receives such requests from “network application servers.”
- At least as to claim 1, Headwater fails to identify a “network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests.” Because Headwater does not identify the “multiple requests to transmit application data,” Headwater necessarily fails to identify how any claimed “network message server” can generate corresponding Internet data messages based on said requests. At least with respect to the Samsung Knox Manage ecosystem, Headwater also provides no evidence to identify a message transmitted within said system that contains at least one application identifier for an indicated application and application data corresponding to one of the requests.
- At least as to claim 1, Headwater fails to identify a “network message server [configured] to transmit each of the generated Internet data messages to the device messaging agent based on the device indicated in the corresponding request, using the corresponding secure Internet data connection for the device indicated in the corresponding request.” Headwater fails to explain how the generated Internet data messages can be transmitted from an alleged network message server to the device messaging agents using the secure Internet data connection, since the device messaging agents and the secure Internet data connection are unidentified. To the extent that Headwater contends that the FCM client app constitutes a “device messaging agent,” Headwater further fails to identify a “network message server” that communicates with the FCM client app. Further, the claim requires that the network message server is configured for several functions, including receiving requests from network application servers, generating corresponding Internet data messages based on the requests, and transmitting the corresponding Internet data messages to a device messaging agent based on the data in the request. Headwater provides no evidence to demonstrate that the “Samsung’s push messaging servers” and the “Samsung Knox servers managing



November 22, 2023

Page 7

those phones and devices [enrolled in the Samsung Knox MDM platform]” perform all three above-described functions.

- At least as to claim 1, Headwater fails to identify “each device messaging agent, when executing, [is configured] to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent.” As explained above, the device messaging agents and the secure Internet data connection remain unidentified, and, to the extent that Headwater contends that the FCM client app constitutes a “device messaging agent,” Headwater has failed to identify a “network message server” that communicates with the FCM client app.
- At least as to claim 1, Headwater fails to identify how the accused network system “for each received message, map[s] the application identifier in the message to a software process corresponding to the application identifier, and forward[s] the application data in the message to the software process via a secure interprocess communication service.” Headwater does not identify in its chart how any accused “application identifiers” are mapped to a “software process.” Headwater also cites no evidence to identify the accused “secure interprocess communication service.”

### **3. U.S. Patent No. 9,615,192**

- At least as to claim 1, Headwater fails to disclose how the accused “network link server” comprises “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device.” Headwater does not identify what in the “Samsung push messaging servers” and the “Knox servers” constitutes the claimed transport stack. Headwater further fails to identify how a “respective secure message link” is maintained between the “message link server” and a “device link agent” on a “wireless end-user device[].” Additionally, Headwater fails to identify what constitutes the “device link agent” on an end-user device, and also fails to identify the “multiple software components [on an end-user device] authorized to receive and process data from secure message link messages received via a device link agent on that device.”
- At least as to claim 1, Headwater fails to disclose how the accused “message link server” comprises “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components.” Headwater



November 22, 2023

Page 8

does not identify any such interface to meet this limitation. Headwater thus necessarily does not identify any “network element messages” to be received at said interface.

- At least as to claim 1, Headwater does not disclose its theory as to how the accused “message link server” comprises “a message buffer system including a memory and logic.” Headwater does not point to any particular component of the accused “Samsung push messaging servers” and “Knox servers” as meeting the claimed “memory” and “logic.”
- At least as to claim 1, Headwater fails to disclose its theory as to how the accused “message link server” comprises a “memory” that “buffer[s] content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices.” As explained above, Headwater has failed to identify a “memory,” and, even if Headwater has adequately accused a “memory,” Headwater has failed to identify a “memory” that has buffering capabilities to meet this claim limitation.
- At least as to claim 1, Headwater fails to disclose its theory as to how the accused “message link server” comprises a “logic” that “determine[s] when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs.” As explained above, Headwater has failed to identify a “logic,” and, even if Headwater has adequately accused a “logic,” Headwater has failed to identify a “logic” that has trigger determination capabilities to meet this claim limitation. Headwater also fails to identify what it accuses as the claimed “message delivery triggers.” Headwater further fails to identify where the accused “logic” determines that “the receipt of [a network element message] by the message buffer system” is not a trigger.” Headwater additionally fails to identify what constitutes “an asynchronous event with time-critical messaging needs,” and how said asynchronous event constitutes a trigger.
- At least as to claim 1, Headwater fails to identify how the accused “message link server” comprises “logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices” “upon determining that one of the message delivery triggers has occurred.” As explained above, Headwater has failed to identify a “logic,” and, even if Headwater has adequately accused a “logic,” Headwater has failed to identify a “logic” that supplies messages comprising the buffered content to meet this claim limitation. Further, Headwater fails to disclose its theory as to how this claim limitation is met, because the “secure message link,” the “transport services stack,” the “device link agent,” and the “message delivery triggers” are all unidentified.



November 22, 2023  
Page 9

#### 4. *Dependent Claims*<sup>1</sup>

With respect to the dependent claims, the majority of Headwater's contentions rely on generic cross references to independent claims and fail to disclose Headwater's infringement theories or even explain what portions of the cross-referenced disclosure are supposedly applicable. *See, e.g.*, '733 Chart, at cls. 2-5, 7-14, 19, 21-24, 26, 29; Ex. B to Infr. Conts. re '117 Patent, at cls. 2, 4-6, 9-14, 16-18; Ex. C to Infr. Conts. re '192 Patent, at cls. 3-9, 11-13.

As a non-limiting example, Headwater's contentions for claim 17 of the '117 Patent recite that the Accused Products satisfy the requirement of "wherein the transmission trigger is the expiration of a periodic timer." Yet, Headwater only cites its support for claims 1 and 16, which have no similar requirements, and then states that the "transmission trigger may be a time period of inactivity," thus leaving Samsung to guess at Headwater's infringement theory with respect to elements within this asserted claim. Headwater's contentions across most asserted dependent claims follow this same pattern. As a whole, Headwater's broad cross references lack any mappings between claim elements and supposed support and thus fail to explain with particularity or specificity Headwater's infringement theories for these claims, further prejudicing Samsung's ability to prepare its defenses. *See, e.g.*, *Connectel*, 391 F. Supp. 2d at 527-28.

Headwater's contentions also fail to demonstrate how each claim element is present in the accused instrumentalities. For the '733 patent, many dependent claims recite limitations concerning the type of a "particular server" or "message content," but Headwater only proffers conclusory allegations without any support. For example, with respect to claim 2, which recites that "the particular server" comprises a different type of a server (*e.g.*, "a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server")., Headwater states that the FCM servers receive message content from servers that include, "depending on the use case, any of the specific types of servers listed in this limitation." '733 Chart at 75. Problematically, Headwater does not identify a single instance of such "use case," let alone an instance of a particular server that meets any of the claimed servers. For claims 3 and 4, which recite that the message content comprises "information associated with a service usage" (claim 3) and that "information associated with the service usage comprises information about one or more of a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage, a projected service cost overage, a service plan period time duration, a service plan time remaining before end of period, and a service overage" (claim 4), Headwater simply repeats the claim language and states, without any support, that the FCM servers "receive[] message content comprising information associated with service usage." *Id.* at 75-76.

---

<sup>1</sup> On page 2 of Headwater's cover pleading for its infringement contentions, Headwater asserts claim 6 of the '733 Patent, but provides no claim chart for claim 6 in Exhibit A. Headwater confirmed via email on October 31, 2023, that Headwater is not asserting claim 6 of the '733 Patent.



November 22, 2023  
Page 10

For claim 5, which recites that “the message content is based, at least in part, on a user preference,” Headwater speculates the functionalities of the FCM servers. *See id.* at 77 (“The end user device *may* have particular settings and options (selection of which is a user preference) for enabling receipt of push messages for certain applications.”) (emphasis added). For claim 9, which recites that “the message content comprises an agent instruction, a setting value, an agent configuration, or a software update,” Headwater asserts without support that messages received via FCM servers “comprise instructions to the Firebase SDK on the user device to display notifications (i.e., an ‘agent instruction’).” *Id.* at 79. Headwater does not explain what the alleged notifications are or how the unidentified notifications constitute an “agent instruction.” For claims 11 and 12, which recite that the message content comprises “information associated with a service policy” (claim 11) or “service usage accounting information” (claim 12), Headwater asserts without support that message content received via FCM comprise information associated with service policies/service usage. *Id.* at 81-82. Headwater does not even explain what the alleged “information” is or how it constitutes “service policy” or “service usage accounting information” is. Worse, for claims 8, 10, 14, 19, 22, and 29, Headwater’s contentions are silent on FCM.

Additionally, Headwater’s contentions for claim 4 of the ’192 Patent recite that the accused instrumentalities satisfy the requirement of “wherein the device link agent executes in a secure execution environment on at least one of the devices, and at least one of the software components executes outside of the secure execution environment on that device.” Headwater points to the Secure Folder partition (the Knox Secure Folder), and then states that “[a]pplications stored in the Secure Folder partition are managed separately with respect to push notifications” from applications stored outside of the Secure Folder partition. Nevertheless, Headwater fails to identify any device link agent that executes within the Secure Folder partition, thus leaving Samsung to guess at Headwater’s infringement theory with respect to elements within this asserted claim.

## **II. Headwater’s Contentions Fail to Provide the Disclosures Required by the Patent Rules**

P.R. 3-1(d) requires that Headwater’s contentions disclose “[w]hether each element of each asserted claim is claimed to be literally present or present under the doctrine of equivalents in the Accused Instrumentality.” Headwater, instead, purports to include a mere reservation of rights to later assert infringement under the doctrine of equivalents (“DOE”). Such a reservation of rights is improper. *Godo Kaisha IP Bridge 1 v. Broadcom Ltd.*, No. 2:16-cv-134, 2017 WL 2869331, at \*2 (E.D. Tex. Apr. 27, 2017) (rejecting plaintiff’s argument that its “boilerplate reservation [of the doctrine of equivalents] provides adequate notice under the Local Rules”); *Eolas Techs. Inc. v. Amazon.com, Inc.*, No. 6:15-cv-01038, 2016 WL 7666160, at \*3 (E.D. Tex. Dec. 5, 2016) (striking “boilerplate” doctrine of equivalents infringement contention and holding that “Plaintiff’s boilerplate language also does not reserve any special right for Plaintiff to assert DOE contentions at a time of its choosing”); *see also Biscotti Inc. v. Microsoft Corp.*, No. 2:13-cv-1015, 2017 WL 2267283, at \*4 (E.D. Tex. May 24, 2017) (ruling that “a blanket or boilerplate statement (not tied to any particular claim element) such as ‘any element not literally met is met by the doctrine of equivalents’” is not sufficient to survive a motion to strike). Samsung thus understands that



November 22, 2023  
Page 11

Headwater has no theories of infringement under DOE and no plans to assert any such theories later in the case.

P.R. 3-1(f) requires that “[i]f a party claiming patent infringement wishes to preserve the right to rely, for any purpose, on the assertion that its own apparatus, product, device, process, method, act, or other instrumentality practices the claimed invention, the party must identify, separately for each asserted claim, each such apparatus, product, device, process, method, act, or other instrumentality that incorporates or reflects that particular claim.” Headwater’s contentions merely contend that “ItsOn software **may** incorporate or reflect [unidentified] claims of the Asserted Patents...,” followed by a reservation of rights to later supplement its contentions based on Headwater’s further discovery and investigation. This is improper. If Headwater intended to rely on an assertion that software developed by its related entity, ItsOn, practiced any claims, it should have all the information it needs at this stage to properly disclose such intended reliance in accordance with the Patent Rules. Headwater failed to do so. If Headwater has no ItsOn code that it intends to produce in this case, it should confirm that it does not intend to rely on ItsOn software in stating its claim for infringement.

P.R. 3-2(b) requires that Headwater produce, at this time, “documents evidencing the conception, reduction to practice (‘RTP’), design, and development of each claimed invention.” Headwater produced no such documents but appears to improperly reserve the rights to do so later. Headwater had ample opportunity to diligently search for any such documents in order to produce them by the infringement contentions deadline. Samsung understands that Headwater has no such documents and will not rely in this case on any documents evidencing earlier conception/RTP.

### **III. Identification of Accused Instrumentalities**

Our review of the identified Accused Instrumentalities across the Asserted Patents indicates that Headwater is accusing the same products across all Asserted Patents. Please let us know if we have misread your disclosure.

Headwater improperly attempts to extend its identification of Accused Instrumentalities to other “similar” products. It was Headwater’s obligation to identify with specificity in its infringement contentions the Accused Instrumentalities it plans to target in this case. P.R. 3-1(b). Samsung understands that the complete list of Accused Instrumentalities is comprised of those specifically identified in Headwater’s contentions. If Headwater intended to accuse additional publicly-known products, it could have named them.

### **IV. Conclusion**

The foregoing are only exemplary deficiencies in Headwater’s contentions. Such deficiencies fail to give Samsung adequate notice and prejudice Samsung’s ability to timely develop its defenses, including invalidity contentions under P.R. 3-3 and to identify potential claim construction disputes. Samsung reserves the right to identify additional deficiencies in



November 22, 2023  
Page 12

Headwater's contentions as the case develops and Samsung continues to consider Headwater's infringement allegations. Samsung also reserves the rights to strike or preclude evidence or assertions later introduced by Headwater. Headwater must promptly amend its contentions to include the necessary specificity to bring Headwater's contentions in compliance with the District's Patent Local Rules and avoid further prejudice to Samsung.

Please confirm that Headwater will amend its contentions no later than November 28, 2023, to address these deficiencies.

Regards,

A handwritten signature in black ink, appearing to read "Thad C. Kodish".

Thad C. Kodish



November 22, 2023

Page 13

## **Appendix A – Theories Headwater Dropped in its Infringement Contentions**

### **'733 Patent**

- “As a further example, the communications link Samsung Knox Manage servers or Knox MDM platform and devices being managed by such servers or MDM platform, for example including the Knox workspace devices, Android devices, iOS devices, Chrome OS devices, and Windows devices illustrated above, comprise a ‘service control link.’ Data and messages transmitted over the secure control link between the Samsung Knox Manage servers or Knox MDM platform and managed devices is encrypted, and commands and notifications transmitted from such servers to devices are ‘agent messages.’” *Compare '733 Chart at 12 with ECF No. 31-4 at 12-13.*
- “As a further example, the communications link between Samsung's Tizen servers and Tizen OS devices, and Firebase messaging servers and Samsung's Android devices, comprises a ‘service control link.’ Notifications, data, and messages transmitted over these service control links from such servers to devices are encrypted, as illustrated above, and are ‘agent messages.’” *Id.*
- “As a further example, Samsung's Knox MDM platform, Knox Manage servers and Tizen servers are all examples of servers which provide control plane communications and which are service control server link elements, including because they control, manage, and apply service policies to user devices to which they are connected.” *Id.*
- “As a further example, devices managed by Samsung Knox Manage or the Knox MDM platform are managed by software including specific end-user device applications and software, such as the Knox Manage (KM) agent on such devices (see, e.g., <https://docs.samsungknox.com/admin/knox-manage/enroll-a-single-device.htm>).” *Id.*
- “As a further illustration, the service control device link agents on Samsung's devices are coupled to various other device agents within the device by way of the Android operating system through an agent communication bus. That communication structure allows for intercommunication between agents in the device, and enables the service control device link agents to send messages to (and control) behavior of other components within the system. The communications bus connecting device agents to the service control device link agents need not be internal to the device, and the communications channel between Samsung Knox and MDM servers and managed devices is an example of such a communications bus.” *Compare '733 Chart at 23 with ECF No. 31-4 at 24.*

### **'117 Patent:**



November 22, 2023

Page 14

- “As a further example, the communications links between Samsung Knox Manage servers or Knox MDM platform and devices being managed by such servers or MDM platform, for example including the Knox workspace devices, Android devices, iOS devices, Chrome OS devices, and Windows devices illustrated above, comprise secure Internet data connections, in that the connections are secure (insofar as they are encrypted per Samsung’s requirements) and used to transmit information over the Internet. As a further example, the communications link between Samsung’s Tizen servers and Tizen OS devices, and Firebase messaging servers and Samsung’s Android devices, comprises a secure Internet data connections. Like with commands and messages sent between Knox servers and Knox-managed devices, notifications, data, and messages transmitted over these communications links in the Tizen and Firebase messaging framework may be encrypted, as illustrated above. See, e.g., (<https://docs.tizen.org/application/native/guides/messaging/push/#security> (“ret = push\_service\_get\_notification\_data(noti, &data); /\* Decrypt app data here if it is encrypted \*/”)).” *Compare ECF No. 31-5 at 31-32 with ’117 Chart at 33.*
- “Each Tizen, Android, and Knox-managed device has an operating system (Tizen OS, Android OS, etc.) in which applications and software agents on the device are able to communicate with one another through the use of a communications bus or “a secure interprocess communication service.” In the case of Android (and Knox-managed) devices, that service may be provided by the Android API; in Tizen devices, it may be provided by the Tizen API used by applications in the Tizen OS (e.g., the mobile and wearable Application APIs, see, e.g., <https://docs.tizen.org/application/native/index>). Messages received by the push service running on Tizen and Android devices, for example, communicate with other applications on the device, including sending notifications to applications that were received via the push service. Likewise, with Knox, messages sent to Knox agents from Knox servers may be authenticated by the user device and passed on to relevant application on the device or, if the application is not installed, causes an application to be installed (see, e.g., <https://docs.samsungknox.com/admin/knoxmanage/add-applications-intro.htm>, <https://docs.samsungknox.com/admin/knox-manage/assigninternal-applications.htm>).” *Compare ECF No. 31-5 at 80 with ’117 Chart at 82.*

**’192 Patent:**

- “As a further example, the communications link Samsung Knox Manage servers or Knox MDM platform and devices being managed by such servers or MDM platform, for example including the Knox workspace devices, Android devices, iOS devices, Chrome OS devices, and Windows devices illustrated above, comprise a “service control link.” Data and messages transmitted over the secure message link between the Samsung Knox Manage servers or Knox MDM platform and managed devices are encrypted, and commands and notifications transmitted from such servers to devices are messages.” *Compare ECF No. 31-6 at 11-12 with ’192 Chart at 12-13.*



November 22, 2023

Page 15

- “As a further example, the communications link between Samsung’s Tizen servers and Tizen OS devices, and Firebase messaging servers and Samsung’s Android devices, comprises a “service message link.” Notifications, data, and messages transmitted over these service control links from such servers to devices are encrypted, as illustrated above, and are messages.” *Compare ECF No. 31-6 at 12 with ’192 Chart at 12-13.*
- “As a further example, the App Servers communicating with Tizen and Firebase notification servers (each a network element) send messages such as notifications (network element messages comprising respective message content and request for delivery of the respective message content), which are routed through Samsung’s Tizen and Knox servers and Google’s Firebase messaging servers. Alternatively, administrator devices communicating with Knox MDM and Knox Manage servers to manage and control devices in the Knox device group are also network elements which send to the Knox servers messages that comprise message content and requests for delivery of the message content down to the managed devices. Such messages can be device commands transmitted from the administrator devices to managed devices via Knox servers (e.g., <https://docs.samsungknox.com/admin/knox-manage/send-commands-todevices.htm>) or readable notifications. Alternatively, each of the managed devices in a Knox MDM group can also comprise network elements sending messages and requests for delivery of message content, for example when agents on the managed device monitor and trigger alerts to be sent to administrator devices via Knox MDM servers ( e.g., <https://docs.samsungknox.com/admin/knox-manage/configure-alerts.htm>). In each example, such messages include data for, and identification of, a respective one of the authorized software components (e.g., the application to which the notification and message is delivered, whether it is the Knox Agent on the devices, the Knox Manage application on the administrator device, or the particular application on the Tizen device receiving a notification).” *Compare ECF No. 31-6 at 18-19 with ’192 Chart at 20-21.*
- “As a further example, Samsung’s Tizen servers and Knox servers are able to deliver commands and messages to devices (such as Tizen OS smartwatches and televisions), Knox-managed devices, and Knox administrator devices when an asynchronous event with time-critical messaging needs is detected within the network. Such events include, for example, the detection of specific events monitored by software at a device (e.g., <https://docs.samsungknox.com/admin/knox-manage/configure-alerts.htm>, and purchase or billing transactions initiated by one device). As another example, an asynchronous event with time-critical messaging needs may be the detection of a device as having been connected to the Internet, Knox servers, or Tizen servers, in which case messages intended for that device are delivered to the device at that point. *Compare ECF No. 31-6 at 49-50 with ’192 Chart at 50.*
- “As a further example, Samsung’s Tizen and Knox products utilize communication layers comprising a transport services stack at the servers and devices to which the servers are connected. As one example, the secure control link between Knox servers and Knox-



November 22, 2023  
Page 16

managed devices communicate through specific software residing on both Knox servers (Knox Manage software) and Knox-managed devices (e.g., Knox agent at the devices) which receives, decrypts and decodes, interprets, and executes commands or messages from other elements in the system. Likewise, with Samsung's Tizen devices, specific software within both Tizen OS and Tizen's push messaging servers operate in a similar fashion." *Compare ECF No. 31-6 at 60 with '192 Chart at 60.*